



Annual 47 C.F.R. § 64.2009(e) CPNI Certification Template EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2015 covering the prior calendar year 2014

1. Date filed: April 11, 2017
2. Name of company covered by this certification: City of Salisbury
3. Form 499 Filer ID(s): 828893
4. Name of signatory: John A. Sofley, Jr.
5. Title of signatory: Assistant City Manager

I, John A. Sofley, Jr., certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. See 47 C.F.R. § 64.2001 et seq.

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements (including those mandating the adoption of CPNI procedures, training, recordkeeping, and supervisory review) set forth in section 64.2001 et seq. of the Commission's rules.

The company has not taken actions (i.e., proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year.

The company has not received customer complaints in the past year concerning the unauthorized release of CPNI.

The company represents and warrants that the above certification is consistent with 47 C.F.R. § 1.17 which requires truthful and accurate statements to the Commission. The company also acknowledges that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may subject it to enforcement action.

Signature John A. Sofley, Jr. Date April 11, 2017

Attachment: Accompanying Statement explaining CNPI procedures

City of Salisbury
5309
Post Office Box 479

Administration
Salisbury, NC 28145-0479

Telephone (704) 638-
Fax (704) 638-8434

City of Salisbury (ID:828893)

OPERATING PROCEDURES FOR COMPLIANCE WITH CPNI RULES

City of Salisbury (the “City”) has implemented the following procedures to ensure that it is compliant with Part 64 of Title 47 of the Code of Federal Regulations, Subpart U – Customer Proprietary Network Information (CPNI), § 64.2001 through § 64.2011.

Compliance Officer

The City has not appointed an official Compliance Officer. The City does appoint a Customer Service Manager whose responsibilities includes making sure that no use of CPNI is made without review of applicable rules and laws.

Employee Training

The Customer Service Manager arranges for the training of all employees on a regular basis, and more frequently as needed. Any new employee is trained when hired by the City. The training includes, but is not limited to, when employees are and are not authorized to use CPNI, and the authentication methods the City is using. After the training, all employees are required to sign a certification that they have received training on the CPNI rules, that they understand the City’s procedures for protecting CPNI and they understand the City’s disciplinary process for improper use of CPNI. Employees are instructed that if they ever have any questions regarding the use of CPNI, if they are aware of CPNI being used improperly by anyone, or if they encounter someone other than the authorized person on an account trying to access CPNI that they should contact the Customer Service Manager immediately. The Customer Service Manager will then determine what actions need to be taken. The City reserves the right to depart from past disciplinary practices at its sole discretion, when it seems such departure is desirable and appropriate.

Customer Notification and Request for Approval to Use CPNI

The City has not provided notification to its customers and has not asked for approval to use CPNI because it only uses CPNI in those instances where it is permissible to use CPNI without customer approval. It does not share the customer’s CPNI with any joint venture partner, independent contractor or any other third party. If the City receives a call from a customer who wants to discuss services outside of the customer’s existing service offerings, the customer service representative uses the oral notification for one-time use of CPNI to obtain approval for the duration of the call only. If, in the future, the City decides to ask customers for approval to use their CPNI, it will implement a system by which the status of a customer’s CPNI approval can be clearly established prior to the use of CPNI.

Marketing Campaigns

The City has not provided notification to its customers and has not asked for approval to use CPNI because it only uses CPNI in those instances where it is permissible to use CPNI without customer approval. It does not share the customer’s CPNI with any joint venture partner, independent contractor or any other third party.

If, in the future, the City decides to ask customers for approval to use their CPNI, it will implement a system by which the status of a customer's CPNI approval can be clearly established prior to the use of CPNI.

Authentication

The City does not disclose any CPNI until the customer has been appropriately authenticated. If the customer cannot provide all of the call detail information to address the customer's issue, the City will ask the customer to come into the office and provide appropriate identification.

Notification of Breaches

Employees will immediately notify the Customer Service Manager of any indication of a breach. If it is determined that a breach has occurred, the Customer Service Manager will do the following:

- Notify the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI) as soon as practicable, but in no event later than 7 business days after determination of the breach. The notification will be via the FCC link at <http://www.fcc.gov/eb/cpni>.
- Notify customers only after 7 full business days have passed since notification to the USSS and the FBI, unless the USSS or FBI has requested an extension. If there is an urgent need to notify affected customers or the public sooner to avoid immediate and irreparable harm, it will be done only after consultation with the relevant investigating agency.
- Maintain a record of the breach, the notifications made to the USSS and FBI, and the notifications made to customers. The record will include dates of discovery and notification, a detailed description of the CPNI that was the subject of the breach, and the circumstances of the breach.
- Include a summary of the breach in the annual compliance certificate filed with the FCC.

Record Retention

The City retains all information regarding CPNI. Records are retained as required by Federal and State laws.